⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平1−253051

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　平成1年(1989)10月9日
G 06 F 12/14	320	B−7737−5B	
9/06	450	A−7361−5B	
G 09 C 1/00	310	7368−5B	審査請求　未請求　請求項の数 2　(全6頁)

⑤4発明の名称　情報保護方法

⑳特　願　昭63−80001
㉒出　願　昭63(1988)3月31日

⑦2発明者　力石　徹也　神奈川県高座郡寒川町小谷2丁目1番1号　東洋通信機株式会社内
⑦1出願人　東洋通信機株式会社　神奈川県高座郡寒川町小谷2丁目1番1号

明細書

1.発明の名称

情報保護方法

2.特許請求の範囲

1. 情報を所要数に分割し，該分割した情報のうち所要のものの夫々にその次の情報を指定するための選択情報を付加し，これ等各々を所望の暗号手段によって暗号化したことを特徴とする情報保護方法。
2. 特許請求の範囲第1項に記載した方法によって暗号化した情報を復号化する場合，分割情報各々の暗号手段に対応した復号手段と，所要の復号手段を選択的に接続する複数の転送部とを具え，選択情報に対応した転送部を指定し，その転送部に接続した復号手段によって復号化したことを特徴とする情報保護方法。

3.発明の詳細な説明

(発明の属する分野)

本発明は情報保護方法，殊にプログラム或はデータを所望の暗号手段によって暗号化し正当な利用者のみが暗号化したプログラム或はデータを復号化して使用することができる情報保護方法に関する。

(従来技術)

現在，コンピュータを動作させるのに不可欠なプログラム或はデータはこれをフロッピーディスク等の記憶媒体に書き込んで保存し，必要なときに読み出して使用するのが一般的であるが，フロッピーディスクに書き込んだプログラム或はデータは簡単に他のフロッピーディスクにコピーすることができるため第三者に盗用されてしまう虞れがある。

従来，第三者の盗用を防止し情報，例えばプログラムを保護する方法としては，そのプログラムを所望の暗号手段によって暗号化した後にフロッピーディスクに書き込んで保存し，これを使用するときには使用するプログラムの暗号手段に対応した復号手段に基づいて作成した復号化プログラムを書き込んだROMカートリッ

ジをコンピュータのＲＯＭカートリッジスロットに挿入しその復号化プログラムによって暗号化したプログラムを元に復号化して使用できるようにした方法がある。

この方法によれば，フロッピーディスクに保存したプログラムを第三者が不正に他のフロッピーディスクにコピーしてもこれには暗号化したプログラムがコピーされるため第三者は，コピーしたフロッピーディスクから元のプログラムを得ることが困難であり，盗用を防止してプログラムを保護することができる。

しかしながら，この方法では第三者が暗号化したプログラムに対応するＲＯＭカートリッジを入手してＲＯＭカートリッジスロットに挿入すればフロッピーディスクの暗号化したプログラムを容易に実行することができるためフロッピーディスクを厳重に保管しなければならなかった。

（発明の目的）

本発明は，上述した事情に鑑みてなされたものであって，第三者がＲＯＭカートリッジ等の復号手段を入手しても暗号化したプログラム或はデータ等の情報を使用することが困難な情報保護方法を提供することを目的とする。

（発明の概要）

上述の目的を達成する為本発明の情報保護方法は例えば，プログラムを所望数に分割し，分割プログラム夫々にその次に実行する分割プログラムを指定するための選択情報を付加すると共にこれ等各々を所望の暗号手段によって暗号化し，暗号化した各々の分割プログラムをプログラムの実行順に並べてフロッピーディスクに書き込んで保存する。

又，この暗号化したプログラムを使用する場合は，暗号化した分割プログラム各々の暗号手段に応じた復号手段を夫々所定の転送部に選択的に接続することによって，各々の分割プログラム毎に選択情報に応じた転送部を指定し，指定した転送部に接続した復号手段によって暗号化した分割プログラムを復号化し元のプログラムを得るように手段を講ずる。

（実施例）

以下，本発明を図面に示した実施例に基づいて詳細に説明する。

第１図は本発明に係る暗号手段の一実施例を示すフローチャート図である。

先ず，保護するプログラムをメモリに書き込み，キーボードからそのプログラムを分割する数を入力し，その入力数に従って保護するプログラムをメモリアドレスによって分割して前記入力した数の分割プログラムを得る。次にキーボードから，分割プログラム各々に対して暗号手段の種類を選択すると共にその各々の暗号手段に応じた復号手段を指定する情報を入力する。このキー入力に基づいて各分割プログラムは，その実行順に次に実行する分割プログラムの有無を判断する即ち，最後に実行する分割プログラムか否かを判断する。この判断によって，次に実行する分割プログラムが有る場合はその分割プログラムに，次に実行する分割プログラムの復号手段を指定する選択情報を付加すると共に，これをキー入力時に選択した暗号手段によって暗号化する。又，最後に実行する分割プログラムの場合はその分割プログラムをキー入力時に選択した暗号手段によって暗号化する。このような手順に従って，暗号化した分割プログラムはメモリからその実行順にフロッピーディスクに記録して保存する。

次に，暗号化したプログラムを復号化する場合について説明する。

復号化する場合は，予め第２図に示すような暗号化したプログラムを元に復号化する復号手段Ｄ１及びＤ２を選択的に接続するＡＯ乃至Ａｎの転送部を具えると共に各分割プログラムの選択情報に従って所定の転送部を選択する拡張装置Ｉを設ける。

この拡張装置１を使用し，上述の如くフロッピーディスクに保存した暗号化プログラムを復号化するには，第３図に示すフローチャートの手順に従えば良い。先ず，暗号化した分割プログラム各々の暗号手段に応じた復号手段Ｄ１及

びD2を夫々前記分割プログラムの選択情報に応じた転送部に接続する。次に，フロッピーディスクから上述の如く保存したプログラムをメモリに書き込み，キーボードから最初に実行する暗号化した分割プログラムの先頭番地及びこれに応じた選択情報を入力する。キー入力した後，指定した先頭番地の暗号化分割プログラムは，選択情報に応じた転送部の復号手段によって復号化し元の分割プログラムをメモリに書き込む。その後，元の分割プログラムはこれに選択情報が含まれているか否かを判断する。選択情報を含んでいる場合は，その情報に応じて上述のキー入力した後の手順と同様に次に実行する暗号化分割プログラムを前記選択情報に応じた転送部の復号手段によって復号化して元の分割プログラムをメモリに書き込み，再び選択情報が含まれているか否かを判断する。又，選択情報を含んでいない場合は復号化の手順を終了し，元の分割プログラムを復号化した順に実行する。

第4図は，以上説明した手順で動作するコンピュータシステムの一実施例を示す構成図である。

同図に於いて2は各種プログラムに従って演算処理するCPU，3はプログラム或はデータを記憶するためのメモリ，4はこれ等内部と外部との間のプログラム或はデータを転送入出力するための入出力部であって，これ等を互いにアドレスライン，データライン及びコントロールラインによって接続してコンピュータ5を構成する。更に，このコンピュータ5はプログラムの実行状態に従って画面表示するためのCRT6，キー入力するためのキーボード7，プログラムを記録するフロッピーディスク8をアクセスするためのフロッピーディスクドライブ9，暗号化するプログラムを書き込んだ暗号化ROM10，11，及び復号化プログラムを書き込んだ復号化ROM12及び13を接続するための拡張装置14各々を具え，これ等各々と入出力部4との間を所要のラインによって接続してコンピュータシステムを構成する。又，拡張装置14は復号化ROM12及び13を選択的に接続する転送部15−0乃至15−3によって構成する。

上述したコンピュータシステムは以下の如く動作する。

ここでは，保護のするプログラムPを分割プログラムP1乃至P3として3分割し，互いに異なる暗号手段に基づいてプログラミングした暗号化プログラムAS及びBSを夫々暗号化ROM10及び11に書き込む。又，暗号化プログラムASに対応する復号化プログラムADを復号化ROM12に書き込み，これを転送部15−1に接続すると共に，暗号化プログラムBSに対応する復号化プログラムBDを復号化ROM13に書き込み，これを転送部15−3に接続する場合について説明する。

プログラムPを暗号化する場合は第1図に示すフローチャートに基づいてプログラミングした暗号作成プログラムSをフロッピーディスク8からメモリ3にロードして暗号作成プログラムSを実行する。これによってCPU2は，プログラムPをメモリ3にロードしキーボード7からプログラムPを分割する数3を入力しプログラムPをロードしたメモリ領域内に於いて3分割するように分割プログラムP1乃至P3各々のアドレス範囲を定める。その後キーボード7から分割プログラムP1及びP3夫々に対して暗号化ROM10を選択すると共に分割プログラムP2に対して暗号化ROM11を選択し，復号化ROM12及び13を夫々転送部15−1および15−3に接続することに対応した情報を入力する。これによってCPU2は転送部15−3を指定する選択情報S1をメモリ3の空いているメモリ領域に書き込み~~終了後~~，暗号化ROM10から暗号化プログラムASをメモリ3にロードした後実行すると共に，分割プログラムP1と選択情報S1とを所定の暗号手段によって暗号化した暗号分割プログラムC1を作成しかつこれをメモリ3の空いている領域に書き込む。又，CPU2は転送部15−1を指定する選択情報S2をメ

モリ3の空いている領域に書き込んだ後，暗号化ROM11から暗号化プログラムBSをメモリ3にロードした後実行すると共に，分割プログラムP2と選択情報S2とを所定の暗号手段によって暗号化した暗号分割プログラムC2を作成し，これを暗号分割プログラムC1の次のメモリ領域内に書き込む。更に，CPU2は暗号化ROM10から暗号化プログラムASをメモリ3にロードした後実行すると共に，分割プログラムP3を所定の暗号手段によって暗号化した暗号分割プログラムC3を作成し，これを暗号分割プログラムC2の次のメモリ領域内に書き込む。

このようにメモリ3のメモリ領域内に書き込んだ暗号分割プログラムC1乃至C3はキーボード7を操作することによってフロッピーディスク8にセーブして保存する。

次に，上述のように暗号化したプログラムPを元に復号化する場合について説明する。

先ず，復号化ROM12及び13を夫々転送部15−1及び15−3に接続し，フロッピーディスク8からメモリ3に第3図に示すフローチャート図に基づいてプログラミングした解読処理プログラムDをロードして復号処理プログラムDを実行する。これによってCPU2は，フロッピーディスク8から暗号分割プログラムC1乃至C3をメモリ3にロードし，キーボード7から始めに実行する暗号分割プログラムC1の先頭番地を入力すると共にそれに対応する転送部15−1を指定することによって復号化ROM12からメモリ3に復号化プログラムADを書き込みそれを実行し，暗号分割プログラムC1を元に復号化して選択情報S1を付加した分割プログラムP1を得てその選択情報S1を除いた分割プログラムP1をメモリ3の空いている領域に書き込む。次に，CPU2は選択情報S1によって転送部15−3を指定し復号化ROM13からメモリ3に復号化プログラムBDを書き込みそれを実行し，暗号分割プログラムC2を元に復号化して選択情報S2を付加した分割プログラムP2を得てその選択情報S2を除いた分割プログラムP2を上述の選択プログラムS1を除いた分割プログラムP1の次のメモリ領域内に書き込む。更に，CPU2は選択プログラムS2によって転送部15−1を指定し復号化ROM12からメモリ3に復号化プログラムADを書き込みそれを実行し，暗号分割プログラムC3を元に復号化して分割プログラムP3を得てそれを上述の選択情報S2を除いた分割プログラムP2の次のメモリ領域内に書き込む。

このように復号化した後CPU2は，メモリ3の分割プログラムP1乃至P3をその順に実行する。

従って，上述の如く説明した方法によれば第3者が復号化ROM12及び13を入手したとしても夫々を転送部15−1及び15−3以外に接続すると暗号分割プログラムC1乃至C3は，それ等夫々に対応した復号化ROMを接続した転送部を指定し得ないため元の分割プログラムP1乃至P3を得ることができない即ち，プログラムPの不正使用を防止できる。

尚，上述の実施例では分割プログラムを暗号化する場合所望の暗号化プログラムを書き込んだ暗号化ROMを用いたが，本発明はこれに限る必要はなく，例えば第5図に示すように所望の暗号手段に基づいてプログラミングした暗号化プログラムを書き込んだROM16，その暗号化プログラムに従って実行処理をするためのCPU17，コンピュータからの分割プログラムを記憶するためのRAM18及びコンピュータと接続するための入出力部19とを具えた暗号化装置20を用いても良い。これは，コンピュータからRAM18に所要の分割プログラムを転送することによって，これに応じた暗号分割プログラムをROM16の暗号化プログラムに従って作成しこれをRAM18の空いているメモリ領域に書き込むと共にその暗号分割プログラムをコンピュータに転送するものである。これによれば暗号化プログラムをコンピュータのメモリに書き込む必要がないため第三者から暗号手段の盗

用を防止する上で都合が良いであろう。又，上述の暗号化装置20はROM16に所望の復号手段に基づいてプログラミングした復号化プログラムを書き込み，これを所定の転送部に接続することによって暗号化プログラムを元に復号化することができる復号化装置とすれば，第三者から復号手段の盗用を防止する上で都合が良いであろう。

又，上述の説明では拡張装置に復号化ROM等の復号手段を選択的に接続したが本発明はこれに限る必要はなく，復号手段を選択的に接続可能な場所を複数具えると共にその場所を選択情報に応じて指定するものであれば良い。例えばコンピュータの入出力部に復号手段を選択的に接続し，選択情報に応じて所定の入出力部のポートアドレスを指定するようにしても良い。

更に，本発明は上述のように所望の暗号化手段によって暗号化した分割プログラムを元のプログラムの実行順に保存したが，これに限る必要はない。又，暗号化した分割プログラムを所要数合成しこれを再び所望の暗号手段によって暗号化すれば暗号強度を増す上で都合が良いであろう。

本発明の実施例ではコンピュータにモニタ，キーボード及びフロッピーディスクドライブを接続したがこれに限らず利用者の目的に沿う種々の外部装置を選択すれば良い。又，暗号化するものはプログラム以外にデータであっても良く，これを記録するものもフロッピーディスク以外に磁気テープ或はRAMカード等の記録媒体であれば良いこと自明であろう。

（発明の効果）

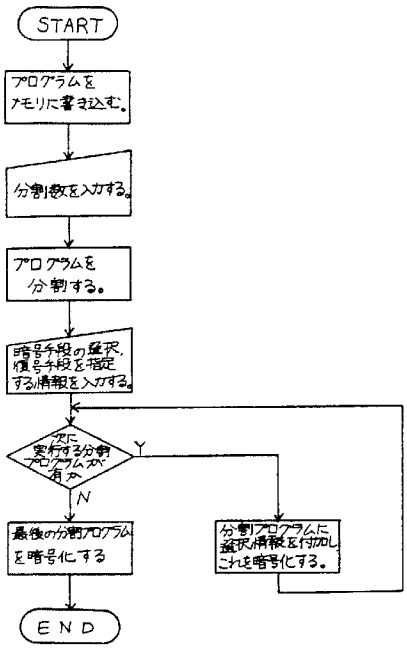
本発明は以上説明したように，保護するプログラム或はデータを所要数に分割した後，各々のプログラム或はデータを所望の暗号手段によって暗号化して保存し，プログラム或はデータを使用する場合は所要の解読手段を所定の転送部に接続することによってプログラムの実行或はデータのアクセスを可能にしたものであるから，復号手段を入手しただけの第三者による不正使用を防止し，情報を保護する上で効果がある。

4.図面の簡単な説面

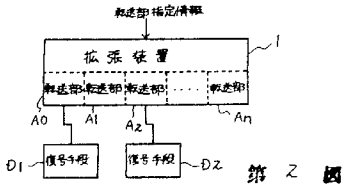
第1図は本発明に係るプログラムを暗号化する場合の一実施例を示すフローチャート図，第2図は本発明に係る拡張装置の一実施例を示す構成図，第3図は本発明に係る暗号化したプログラムを元に復号化する場合の一実施例を示すフローチャート図，第4図は本発明に係るコンピュータシステムの一実施例を示す構成図，第5図は暗号化装置の他の実施例を示す構成図である。

A0乃至An……転送部，　D1，D2……復号手段，　1……拡張装置，　2……CPU，　3……メモリ，　4……入出力部，　5……コンピュータ，　6……CRT，　7……キーボード，　8……フロッピーディスク，　9……フロッピーディスクドライブ，　10，11……暗号化ROM，　12，13……復号化ROM，　14……拡張装置，　15－0乃至15－3……転送部，　16……ROM，　17……CPU，　18……RAM，　19……入出力部，　20……暗号化装置。

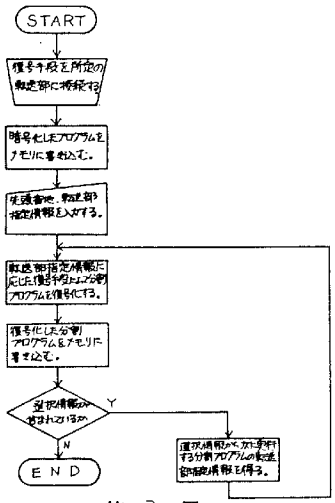
特許出願人　　東洋通信機株式会社



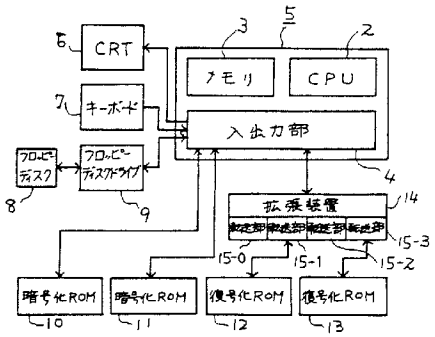
第 1 図



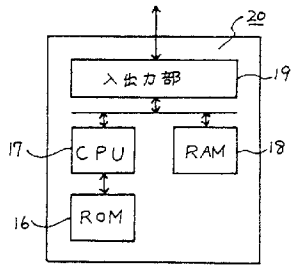
第 2 図



第 3 図



第 4 図



第 5 図